

**UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS**

<p>JENNIFER SHEETS and MICHELLE WILLIAMS, on behalf of themselves and all others similarly situated,</p> <p style="text-align: center;">Plaintiffs,</p> <p style="text-align: center;">v.</p> <p>MEDICAL EYE SERVICES, INC. d/b/a MESVISION and PROGRESS SOFTWARE CORPORATION,</p> <p style="text-align: center;">Defendants.</p>	<p>Case No.: _____</p> <p>CLASS ACTION COMPLAINT</p> <p>DEMAND FOR JURY TRIAL</p>
---	---

Plaintiffs, Jennifer Sheets and Michelle Williams ("Plaintiffs"), individually and on behalf of all similarly situated persons, allege the following against Defendant Medical Eye Services, Inc. d/b/a MESVision ("MESVision") and Defendant Progress Software Corporation ("PSC") (collectively, "Defendants") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by their counsel and review of public documents, as to all other matters:

INTRODUCTION

1. Plaintiffs bring this class action against Defendants for their failure to properly secure and safeguard Plaintiffs' and other similarly situated individuals' sensitive information, including their full names, dates of birth, addresses, Social Security numbers, group IDs, and subscriber IDs ("personally identifiable information" or "PII").

2. Defendant MESVision is a California-based corporation that "provide[s] vision care plans directly to thousands of employer group and millions of plan members nationwide for

leading health care organizations, insurance carriers, and self-funded employer group.”¹

3. Defendant PSC advertises itself as an “experienced, trusted provider of products designed with you, our customers, in mind. With Progress, you can build what you need, deploy where and how you want, empower your customers, then manage it all safely and securely.”²

4. Upon information and belief, former and current users of MESVision’s services are required to entrust Defendants with sensitive, non-public PII, without which Defendants could not perform their regular business activities, in order to obtain eye care services from MESVision. Defendants retain this information for at least many years and even after the relationship has ended.

5. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiffs and Class Members, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

6. On August 23, 2023, MESVision learned that Pension Benefit Information, LLC’s network, which PSC provided software services to and MESVision relied on for the sending and receiving of sensitive information, had been penetrated by a cyberattack.³ In response, MESVision “launched an investigation into the incident, and engaged a cybersecurity firm.”⁴ As a result of the investigation, MESVision concluded—on an undisclosed date—that “the unauthorized individual exfiltrated information from the server on May 28, 2023, and May 31, 2023.”⁵

7. According to the Notice of Data Security Incident letter sent by MESVision, on behalf of Defendants, to Plaintiffs and other victims of the Data Breach (the “Notice Letter”), the

¹ <https://www.mesvision.com/aboutUs>

² <https://www.progress.com/company>

³ The “Notice Letter”. A sample copy is available at <https://apps.web.maine.gov/online/aeviewer/ME/40/769f046d-7eb4-490d-b1f3-5d756ad8eda2.shtml>

⁴ *Id.*

⁵ *Id.*

compromised PII included individuals' full names, dates of birth, addresses, Social Security numbers, group IDs, and subscriber IDs.⁶

8. Defendants failed to adequately protect Plaintiffs' and Class Members PII—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII was compromised due to Defendants' negligent and/or careless acts and omissions and their utter failure to protect consumers' sensitive data. Hackers targeted and obtained Plaintiffs' and Class Members' PII because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

9. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendants' failure to: (i) adequately protect the PII of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendants' inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendants' conduct amounts at least to negligence and violates federal and state statutes.

10. Defendants disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures and ensure those measures were followed by their IT vendors to ensure that the PII of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiffs and Class Members was compromised through disclosure to an

⁶ *Id.*

unknown and unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

11. Plaintiffs and Class Members have suffered injury as a result of Defendants' conduct. These injuries include: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) Plaintiff Sheets' PII being disseminated on the dark web, according to CreditKarma; (ix) statutory damages (x) nominal damages; and (xi) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

12. Plaintiffs seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendants' inadequate data security practices.

PARTIES

13. Plaintiff, Jennifer Sheets, is, and at all times mentioned herein was, an individual and citizen of Ambler, Pennsylvania.

14. Plaintiff, Michelle Williams, is, and at all times mentioned herein was, an individual and citizen of Yonkers, New York.

15. Defendant, Medical Eye Services, Inc. d/b/a MESVision, is a corporation incorporated under the state laws of California with its principal place of business located in Foothill Ranch, California.

16. Defendant, Progress Software Corporation, is a Delaware corporation and maintains its headquarters and principal place of business at 15 Wayside Road, 4th Floor, Burlington, Massachusetts 01803.

JURISDICTION AND VENUE

17. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of interest and costs. The number of class members is over 100, many of whom reside outside the state of Massachusetts and have different citizenship from Defendants, including Plaintiffs. Thus, minimal diversity exists under 28 U.S.C. §1332(d)(2)(A)

18. This Court has jurisdiction over Defendants because Defendants operate in this District.

19. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Defendant PSC's principal place of business is located in this District, a substantial part of the events giving rise to this action occurred in this District, and Defendants have harmed Class Members residing in this District.

FACTUAL ALLEGATIONS

Defendants' Businesses

20. Defendant MESVision is a "consumer activation company" that provides products and/or services to "healthcare organizations" and other companies.⁷

⁷ <https://www.linkedin.com/company/MESVision-inc-/>

21. Defendant PSC advertises itself as an “experienced, trusted provider of products designed with you, our customers, in mind. With Progress, you can build what you need, deploy where and how you want, empower your customers, then manage it all safely and securely.”⁸

22. Plaintiffs and Class Members are current and former users of MESVision healthcare services.

23. As a condition of obtaining benefits at MESVision, Plaintiffs and Class Members were required to entrust Defendants, directly or indirectly, with highly sensitive personal information.

24. The information held by Defendants in their computer systems or those of their vendors at the time of the Data Breach included the unencrypted PII of Plaintiffs and Class Members.

25. Upon information and belief, MESVision made promises and representations to the individuals who use MESVision’s services, including Plaintiffs and Class Members, that the PII collected from them as a condition of obtaining benefits at MESVision would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendants would delete any sensitive information after they were no longer required to maintain it.

26. Indeed, MESVision’s Privacy Policy provides that:

We want the Users' Business Information to remain as secure as reasonably possible. We combine industry-standard technical safeguards with training for those employees who are permitted to access our customers' Business Information. When Users purchase a product or service online, we use Secure Sockets Layer (SSL) and Transport Layer Security (TLS) encryption to encrypt their information before it is sent to us in order to ensure the integrity and privacy of the information that the Users provide to us via the Internet.

Many of our web-based services are hosted on servers that are co-located at a third-party facility with whom we have a contract providing for security measures. For example,

⁸ <https://www.progress.com/company>

hosted services data is submitted via SSL and TLS encryption and stored on a server equipped with industry standard firewalls.

Hosted data may include personally identifiable information and other information that belongs to our customers' own customers, website visitors, or other users. We will not review, share, distribute, or reference any such customer data except as provided in the service, or as may be required by law. Individual records of customer data may be viewed or accessed by authorized MESVision employees, or independent contractors only for the purpose of resolving a problem, support and service for the plan, or suspected violation of the service or license agreement, or as may be required by law. MESVision policy requires that both employees and consultants execute a confidentiality agreement before working for and with MESVision. Those employees that violate our Privacy Policy are subject to disciplinary action, up to and including termination.

...

Data flowing to and from this Site is protected by encrypted digital certificates secured using TLS protocol.⁹

27. Plaintiffs and Class Members provided their PII, directly or indirectly, to Defendants with the reasonable expectation and on the mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

28. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiffs and Class Members relied on the sophistication of Defendants to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

29. Defendants had duties to adopt reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to third parties, and MESVision had a duty to audit, monitor, and verify the integrity of its IT vendors and affiliates. Defendants have a legal

⁹ <https://www.mesvision.com/legal/privacy>

duty to keep consumer's PII safe and confidential.

30. Defendants had obligations created by FTC Act, HIPAA, contract, industry standards, and representations made to Plaintiffs and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

31. Defendants derived a substantial economic benefit from collecting Plaintiffs' and Class Members' PII. Without the required submission of PII, Defendants could not perform the services they provide.

32. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

The Data Breach

33. On or about November 14, 2023, MESVision, on behalf of Defendants, began sending Plaintiffs and other Data Breach victims a Notice of Data Security Incident letter (the "Notice Letter"), informing them that:

What happened? MESVision uses a secure file-transfer program called MOVEit. On August 23, 2023, MESVision discovered that an unauthorized individual had accessed information on its MOVEit server by exploiting a vulnerability in MOVEit's system. MESVision immediately took the server offline, launched an investigation into the incident, and engaged a cybersecurity firm. It was determined that the unauthorized individual exfiltrated information from the server on May 28, 2023, and May 31, 2023. We also reported the incident to the FBI.

What information was involved? The server contained information about individuals who are enrolled in vision benefit plans managed by MESVision. Following a detailed analysis and review of all potentially compromised files, we recently determined that the information affected may have included: date of birth, Social Security number, name, address, group ID, and subscriber ID.¹⁰

34. Omitted from the Notice Letter were any explanation as to why it took MESVision

¹⁰ Notice Letter.

approximately three months to notify Plaintiffs and Class Members of the Data Breach's occurrence after detecting the cyberattack, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their PII remains protected.

35. This “disclosure” amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class Members of the Data Breach’s critical facts. Without these details, Plaintiffs’ and Class Members’ ability to mitigate the harms resulting from the Data Breach is severely diminished.

36. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed. Moreover, MESVision failed to exercise due diligence in selecting its IT vendors or deciding with whom it would share sensitive PII.

37. The attacker accessed and acquired files from Defendants containing unencrypted PII of Plaintiffs and Class Members, including their Social Security numbers and other sensitive information. Plaintiffs’ and Class Members’ PII was accessed and stolen in the Data Breach.

38. As Plaintiff Sheets has already experienced, the PII of Class Members was or will be subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

Defendants Acquire, Collect, and Store Plaintiff’s and Class Members’ PII

39. As a condition to obtain benefits at MESVision, Plaintiffs and Class Members were required to give their sensitive and confidential PII, directly or indirectly, to Defendants.

40. MESVision retains and stores this information with PSC and derives a substantial economic benefit from the PII that they collect. But for the collection of Plaintiffs' and Class Members' PII, Defendants would be unable to perform their services.

41. By obtaining, collecting, and storing the PII of Plaintiffs and Class Members, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII from disclosure.

42. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendants to keep their PII confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

43. Defendants could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiffs and Class Members or by MESVision exercising due diligence in selecting its IT vendors and properly auditing those vendor's security practices.

44. Upon information and belief, Defendants made promises to Plaintiffs and Class Members to maintain and protect their PII, demonstrating an understanding of the importance of securing PII.

45. Indeed, MESVision's Privacy Policy provides that:

We want the Users' Business Information to remain as secure as reasonably possible. We combine industry-standard technical safeguards with training for those employees who are permitted to access our customers' Business Information. When Users purchase a product or service online, we use Secure Sockets Layer (SSL) and Transport Layer Security (TLS) encryption to encrypt their information before it is sent to us in order to ensure the integrity and privacy of the information that the Users provide to us via the Internet.

Many of our web-based services are hosted on servers that are co-located at a third-party facility with whom we have a contract providing for security measures. For example,

hosted services data is submitted via SSL and TLS encryption and stored on a server equipped with industry standard firewalls.

Hosted data may include personally identifiable information and other information that belongs to our customers' own customers, website visitors, or other users. We will not review, share, distribute, or reference any such customer data except as provided in the service, or as may be required by law. Individual records of customer data may be viewed or accessed by authorized MESVision employees, or independent contractors only for the purpose of resolving a problem, support and service for the plan, or suspected violation of the service or license agreement, or as may be required by law. MESVision policy requires that both employees and consultants execute a confidentiality agreement before working for and with MESVision. Those employees that violate our Privacy Policy are subject to disciplinary action, up to and including termination.

...

Data flowing to and from this Site is protected by encrypted digital certificates secured using TLS protocol.¹¹

46. Defendants' negligence in safeguarding the PII of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

E. Defendants Knew or Should Have Known of the Risk Because Eye Care Companies and Software Companies In Possession Of PII Are Particularly Susceptable To Cyber Attacks

47. Data thieves regularly target companies like Defendants' due to the highly sensitive information that they custody. Defendants knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

48. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting eye care companies and software companies that collect and store PII, like Defendants, preceding the date of the breach.

¹¹ <https://www.mesvision.com/legal/privacy>

49. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.¹²

50. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendants knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

51. Indeed, cyber-attacks, such as the one experienced by Defendants, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store PII are "attractive to ransomware criminals...because they often have lesser IT defenses and a high incentive to regain access to their data quickly."¹³

52. Additionally, as companies became more dependent on computer systems to run their business,¹⁴ e.g., working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.¹⁵

53. As custodians of PII, Defendants knew, or should have known, the importance of

¹² See <https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/>

¹³ https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection

¹⁴ <https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html>

¹⁵ <https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022>

safeguarding the PII entrusted to it by Plaintiffs and Class members, and of the foreseeable consequences if their data security systems were breached, including the significant costs imposed on Plaintiffs and Class Members as a result of a breach.

54. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

55. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members and of the foreseeable consequences that would occur if Defendants' data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

56. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' servers, amounting to more than three hundred thousand individuals' detailed PII,¹⁶ and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

57. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

58. The ramifications of Defendants' failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

¹⁶ <https://apps.web.maine.gov/online/aeviewer/ME/40/769f046d-7eb4-490d-b1f3-5d756ad8eda2.shtml>

59. In the Notice Letter, MESVision offers to cover credit and identity theft monitoring services for Plaintiffs and Class Members. This is wholly inadequate to compensate Plaintiffs and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' PII. Moreover, once this service expires, Plaintiffs and Class Members will be forced to pay out of pocket for necessary identity monitoring services.

60. MESVision's offer of credit and identity monitoring establishes that Plaintiffs' and Class Members' sensitive PII *was* in fact affected, accessed, compromised, and exfiltrated from Defendant's, or its vendors, computer systems.

61. As an eye care company and a software company in possession of individuals' (who used MESVision's services) PII, Defendants knew, or should have known, the importance of safeguarding the PII entrusted to them by Plaintiffs and Class Members and of the foreseeable consequences if their data security systems, or those on which it transferred PII, were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Nevertheless, Defendants failed to take adequate cybersecurity measures to prevent the Data Breach.

Value Of PII

62. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."¹⁷ The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other

¹⁷ 17 C.F.R. § 248.201 (2013).

things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.”¹⁸

63. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.¹⁹

64. For example, PII can be sold at a price ranging from \$40 to \$200.²⁰ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.²¹

65. Social Security numbers are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual’s Social Security number, as experienced by Plaintiffs and some Class Members, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don’t pay the bills, it damages your credit. You may not find out that someone is using your number until you’re turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.²²

¹⁸ *Id.*

¹⁹ *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/>

²⁰ *Here’s How Much Your PII Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>

²¹ *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> .

²² Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf>

66. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

67. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."

68. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—names, dates of birth, and Social Security numbers.

69. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."²³

70. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

71. The fraudulent activity resulting from the Data Breach may not come to light for

²³ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>

years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.²⁴

Defendants Failed to Comply with FTC Guidelines

72. The Federal Trade Commission (“FTC”) has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company’s failure to maintain reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair practice” in violation of Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

73. In October 2016, the FTC updated its publication, Protecting PII: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal consumer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network’s vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone

²⁴ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf>

is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

74. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

75. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

76. These FTC enforcement actions include actions against eye care companies and software companies, like Defendants.

77. As evidenced by the Data Breach, Defendants failed to properly implement basic data security practices, and MESVision failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

78. Defendants were at all times fully aware of their obligations to protect the PII of the consumers in their networks yet failed to comply with such obligations. Defendants were also aware of the significant repercussions that would result from their failure to do so.

MESVision Failed to Comply with HIPAA Guidelines

79. MESVision is a covered entity under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E (“Standards for Privacy of Individually Identifiable Health Information”), and Security Rule (“Security Standards for the Protection of Electronic Protected Health Information”), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

80. MESVision is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act (“HITECH”).²⁵ See 42 U.S.C. §17921, 45 C.F.R. § 160.103.

81. HIPAA’s Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

82. HIPAA’s Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

83. HIPAA requires “compl[iance] with the applicable standards, implementation specifications, and requirements” of HIPAA “with respect to electronic protected health information.” 45 C.F.R. § 164.302.

84. “Electronic protected health information” is “individually identifiable health information ... that is (i) transmitted by electronic media; maintained in electronic media.” 45 C.F.R. § 160.103.

85. HIPAA’s Security Rule requires MESVision to do the following:

²⁵ HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

- a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;
- b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and
- d. Ensure compliance by its workforce.

86. HIPAA also requires MESVision to “review and modify the security measures implemented ... as needed to continue provision of reasonable and appropriate protection of electronic protected health information.” 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to “[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights.” 45 C.F.R. § 164.312(a)(1).

87. HIPAA and HITECH also obligated MESVision to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

88. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires MESVision to provide notice of the Data Breach to each affected individual “without unreasonable

delay and *in no case later than 60 days following discovery of the breach.*”²⁶

89. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

90. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

91. HIPAA also requires the Office of Civil Rights (“OCR”), within the Department of Health and Human Services (“HHS”), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, “HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule.” US Department of Health & Human Services, Security Rule Guidance Material.²⁷ The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says “represent the industry standard for good business practices with respect to standards for securing e-PHI.” US Department of Health & Human Services, Guidance on Risk Analysis.²⁸

²⁶ Breach Notification Rule, U.S. Dep’t of Health & Human Services, <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html> (emphasis added).

²⁷ <http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html>.

²⁸ <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html>

Defendants Failed to Comply with Industry Standards

92. As noted above, experts studying cybersecurity routinely identify eye care companies and software companies as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

93. Some industry best practices that should be implemented by eye care companies and software companies dealing with sensitive PII, like Defendants, include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendants failed to follow some or all of these industry best practices.

94. Other best cybersecurity practices that are standard in the eye care and software industries include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendants failed to follow these cybersecurity best practices.

95. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

96. Defendants failed to comply with these accepted standards in the eye care and

software industries, thereby permitting the Data Breach to occur.

Defendants Breached Their Duties to Safeguard Plaintiffs' and the Class's PII

97. In addition to their obligations under federal and state laws, Defendants owed duties to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed duties to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems, networks, and protocols adequately protected the PII of Class Members

98. Defendants breached their obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and data, and MESVision failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;
- b. Failing to adequately protect MESVision's consumers' PII;
- c. Failing to properly monitor their own data security systems for existing intrusions;
- d. Failing to sufficiently train their employees and vendors regarding the proper handling of MESVision's consumers' PII;
- e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;
- f. Failing to adhere to HIPAA guidelines and industry standards for cybersecurity as

discussed above; and,

- g. Otherwise breaching their duties and obligations to protect Plaintiffs' and Class Members' PII.

99. Defendants negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' PII by allowing cyberthieves to access their computer networks and systems which contained unsecured and unencrypted PII.

100. Had Defendants remedied the deficiencies in their information storage and security systems or those of their vendors and affiliates, followed industry guidelines, and adopted security measures recommended by experts in the field, they could have prevented intrusion into their information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential PII.

Common Injuries & Damages

101. As a result of Defendants' ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as

Defendant fails to undertake appropriate and adequate measures to protect the PII.

The Data Breach Increases Victims' Risk Of Identity Theft

102. Plaintiffs and Class Members are at a heightened risk of identity theft for years to come.

103. As Plaintiff Sheets has already experienced, the unencrypted PII of Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

104. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

105. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity--or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

106. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can

be the starting point for these additional targeted attacks on the victim.

107. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of “Fullz” packages.²⁹

108. With “Fullz” packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

109. The development of “Fullz” packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs’ and Class Members’ phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

110. The existence and prevalence of “Fullz” packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like driver's license numbers) of

²⁹ “Fullz” is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than MESVision credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even “dead Fullz,” which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a “mule account” (an account that will accept a fraudulent money transfer from a compromised account) without the victim’s knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), [https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-\]\(https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/)

Plaintiffs and the other Class Members.

111. Thus, even if certain information (such as driver’s license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive “Fullz” package.

112. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss Of Time To Mitigate Risk Of Identity Theft And Fraud

113. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

114. Thus, due to the actual and imminent risk of identity theft, MESVision, in its Notice Letter, instructs Plaintiffs and Class Members to take the following measures to protect themselves:

It is always advisable to remain vigilant against attempts at identity theft or fraud, which includes carefully reviewing online and financial accounts, credit reports, and Explanations of Benefits (“EOBs”) from your health insurers for suspicious activity. This is a best practice for all individuals. If you identify suspicious activity, you should contact the company that maintains the account, credit report, or EOB. Additional information about how to protect your identity is contained in Attachment B. Additional information about how to protect your identity is contained in Attachment B.³⁰

115. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as researching and verifying the legitimacy of the Data Breach upon

³⁰ Notice Letter.

receiving the Notice Letter, changing passwords and resecuring their own computer networks, contacting the Social Security Administration to place alerts on their accounts, contacting credit bureaus to place freezes on their accounts, and monitoring their financial accounts and credit reports for any indication of fraudulent activity, which may take years to detect.

116. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”³¹

117. These efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.³²

118. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”³³

Diminution Value Of PII

³¹ See United States Government Accountability Office, GAO-07-737, PII: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

³² See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps>

³³ See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,” p. 2, U.S. Government Accountability Office, June 2007, <https://www.gao.gov/new.items/d07737.pdf> (“GAO Report”).

119. PII is a valuable property right.³⁴ Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

120. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly \$200 billion.³⁵

121. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.^{36,37}

122. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.³⁸

123. Conversely sensitive PII can sell for as much as \$363 per record on the dark web according to the Infosec Institute.³⁹

124. As a result of the Data Breach, Plaintiffs' and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss.

³⁴ See, e.g., Randall T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

³⁵ <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>

³⁶ <https://datacoup.com/>

³⁷ <https://digi.me/what-is-digime/>

³⁸ Nielsen Computer & Mobile Panel, *Frequently Asked Questions*, available at <https://computermobilepanel.nielsen.com/ui/US/en/faqs.html>

³⁹ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>

Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

125. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change, e.g., names, dates of birth, Social Security numbers.

126. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

127. The fraudulent activity resulting from the Data Breach may not come to light for years.

128. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, and of the foreseeable consequences that would occur if Defendants’ data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

129. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants’ networks, amounting to more than three hundred thousand individuals’ detailed personal information, upon information and belief, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

130. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants’ failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

Future Cost of Credit & Identity Theft Monitoring is Reasonable and Necessary

131. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII involved, the volume of data obtained in the Data Breach, and Plaintiff Sheet's PII already being disseminated on the dark web (as discussed below), there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes –e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

132. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

133. Consequently, Plaintiffs and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

134. The retail cost of credit monitoring and identity theft monitoring can cost around \$200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendants' Data Breach.

Loss Of The Benefit Of The Bargain

135. Furthermore, Defendants' poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to accept employment at MESVision's clients, Plaintiffs and other reasonable consumers understood and expected that they were, in part, paying for, or being paid less for, the necessary data security to protect the PII, when in fact,

Defendants did not provide the expected data security. Accordingly, Plaintiffs and Class Members received employment positions that were of a lesser value than what they reasonably expected to receive under the bargains they struck with MESVision's clients.

PLAINTIFFS' EXPERIENCES

Plaintiff Jennifer Sheets

136. Plaintiff Jennifer Sheets is a former employee at Costco, which, upon information and belief, contracted with MESVision for services.

137. As a condition of her employment at Costco, Plaintiff was required to provide her PII, directly or indirectly, to Defendants, including her name, date of birth, Social Security number, and other sensitive information.

138. At the time of the Data Breach—from approximately May 28, 2023 through May 31, 2023—Defendants retained Plaintiff's PII in their systems.

139. Plaintiff Sheets is very careful about sharing her sensitive PII. Plaintiff stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted her PII to Defendants had she known of Defendants' lax data security policies.

140. Plaintiff Sheets received the Notice Letter, by U.S. mail, from MESVision, dated November 14, 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including her name, date of birth, Social Security number, address, group ID, and subscriber ID.

141. As a result of the Data Breach, and at the direction of the Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter,

changing passwords and resecuring her own computer network, and monitoring her credit reports for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant time on reasonable efforts to mitigate the impact of the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

142. Plaintiff suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

143. Plaintiff additionally suffered actual injury in the form of her PII being disseminated on the dark web, according to CreditKarma, which, upon information and belief, was caused by the Data Breach.

144. Plaintiff further suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

145. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about

the Data Breach's occurrence.

146. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

147. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

148. Plaintiff Sheets has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Michelle Williams

149. Plaintiff Michelle Williams is a current employee at Costco, which, upon information and belief, contracted with MESVision for services.

150. As a condition of her employment at Costco, Plaintiff was required to provide her PII, directly or indirectly, to Defendants, including her name, date of birth, Social Security number, and other sensitive information.

151. At the time of the Data Breach—from approximately May 28, 2023 through May 31, 2023—Defendants retained Plaintiff's PII in their systems.

152. Plaintiff Williams is very careful about sharing her sensitive PII. Plaintiff stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted her PII to Defendants had she known of Defendants' lax data security policies.

153. Plaintiff Williams received the Notice Letter, by U.S. mail, from MESVision, dated November 14, 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed

and obtained by unauthorized third parties, including her name, date of birth, Social Security number, address, group ID, and subscriber ID.

154. As a result of the Data Breach, and at the direction of the Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, contacting the Social Security Administration to place an alert on her account, contacting credit bureaus to place freezes on her accounts, and monitoring her financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant time on reasonable efforts to mitigate the impact of the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

155. Plaintiff suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

156. Plaintiff further suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data

Breach.

157. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

158. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

159. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

160. Plaintiff Williams has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

161. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

162. Specifically, Plaintiffs propose the following Class definition, subject to amendment as appropriate:

Nationwide Class

All individuals in the United States whose PII was impacted as a result of the Data Breach (the "Class").

163. Excluded from the Class are Defendants and their parents or subsidiaries, any entities in which it has a controlling interest, as well as their officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

164. Plaintiffs reserve the right to modify or amend the definition of the proposed

Nationwide Class as well as add subclasses, before the Court determines whether certification is appropriate.

165. The proposed Class meet the criteria for certification under Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

166. Numerosity: The Class Members are so numerous that joinder of all members is impracticable. Although the exact number of Class Members is currently unknown to Plaintiffs and exclusively in the possession of Defendants, according to the breach report submitted to the Office of the Maine Attorney General, at least 346,000 persons were impacted in the Data Breach.⁴⁰ The Class is apparently identifiable within Defendants' records, and Defendants have already identified these individuals (as evidenced by MESVision sending them Notice Letters).

167. Commonality: There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Defendants engaged in the conduct alleged herein;
- b. Whether Defendants' conduct violated the FTCA;
- c. When Defendants learned of the Data Breach;
- d. Whether Defendants' response to the Data Breach was adequate;
- e. Whether Defendants unlawfully lost or disclosed Plaintiffs' and Class Members' PII;
- f. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the PII

⁴⁰ <https://apps.web.maine.gov/online/aeviewer/ME/40/769f046d-7eb4-490d-b1f3-5d756ad8eda2.shtml>

compromised in the Data Breach;

- g. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- h. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;
- i. Whether Defendants owed duties to Class Members to safeguard their PII;
- j. Whether Defendants breached their duty to Class Members to safeguard their PII;
- k. Whether hackers obtained Class Members' PII via the Data Breach;
- l. Whether Defendants had legal duties to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class Members;
- m. Whether Defendants breached their duties to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;
- n. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;
- o. What damages Plaintiffs and Class Members suffered as a result of Defendants' misconduct;
- p. Whether Defendants' conduct was negligent;
- q. Whether Defendants were unjustly enriched;
- r. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages;
- s. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and
- t. Whether Plaintiffs and Class Members are entitled to equitable relief, including

injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

168. Typicality: Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII, like that of every other Class Member, was compromised in the Data Breach. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Defendants. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of Class Members arise from the same operative facts and are based on the same legal theories.

169. Adequacy of Representation: Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

170. Predominance: Defendants have engaged in a common course of conduct toward Plaintiffs and Class Members in that all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

171. Superiority: A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high

and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

172. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Defendants have acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

173. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent Notice Letters by MESVision.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class against Defendants)

174. Plaintiffs re-allege and incorporate by reference all preceding paragraphs, as if fully set forth herein, and bring this claim against both Defendants.

175. MESVision requires individuals who use MESVision's services, including Plaintiffs and Class Members, to submit non-public PII to Defendants in the ordinary course of providing its services.

176. Plaintiffs and Class Members entrusted Defendants, directly or indirectly, with their PII with the understanding that Defendants would safeguard their information.

177. Defendants had full knowledge of the sensitivity of the PII and the types of harm

that Plaintiffs and Class Members could and would suffer if the PII were wrongfully disclosed.

178. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendants owed duties of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft. MESVision's duty included a responsibility to exercise due diligence in selecting IT vendors and to audit, monitor, and ensure the integrity of its vendor's systems and practices and to give prompt notice to those affected in the case of a data breach.

179. Defendants had duties to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

180. MESVision's duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

181. For instance, HIPAA required MESVision to notify victims of the Breach within 60 days of the discovery of the Data Breach. MESVision did not begin to notify Plaintiffs or Class Members of the Data Breach until November 14, 2023 despite, upon information and belief, MESVision knowing shortly after August 23, 2023 that unauthorized persons had accessed and acquired the private, protected, personal information of Plaintiffs and the Class.

182. Defendants owed duties of care to Plaintiffs and Class Members to provide data

security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the PII.

183. Defendants' duties of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiffs and Class Members. That special relationship arose because Plaintiffs and the Class entrusted Defendants with their confidential PII, a necessary part of using MESVision's services.

184. Defendants' duties to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential PII.

185. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiffs or the Class.

186. Defendants also had duties to exercise appropriate clearinghouse practices to remove former consumers' PII it was no longer required to retain pursuant to regulations.

187. Moreover, Defendants had duties to promptly and adequately notify Plaintiffs and the Class of the Data Breach.

188. Defendants had and continues to have duties to adequately disclose that the PII of Plaintiffs and the Class within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

189. Defendants breached their duties, pursuant to the FTC Act, HIPAA, and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect

Class Members' PII. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;
- b. Failing to adequately monitor the security of their networks and systems;
- c. Failing to audit, monitor, or ensure the integrity of their vendor's data security practices;
- d. Allowing unauthorized access to Class Members' PII;
- e. Failing to detect in a timely manner that Class Members' PII had been compromised;
- f. Failing to remove former consumers' PII it was no longer required to retain pursuant to regulations,
- g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and
- h. Failing to secure their stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

190. Defendants violated Section 5 of the FTC Act and HIPAA by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

191. Plaintiffs and Class Members were within the class of persons the Federal Trade

Commission Act and HIPAA were intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statutes were intended to guard against.

192. Defendants' violation of Section 5 of the FTC Act and HIPAA constitutes negligence.

193. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

194. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

195. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the eye care and software industries.

196. Defendants have full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Class could and would suffer if the PII were wrongfully disclosed.

197. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendants' systems.

198. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

199. Plaintiffs and the Class had no ability to protect their PII that was in, and possibly remains in, Defendants' possession.

200. Defendants were in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

201. Defendants' duties extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

202. MESVision has admitted that the PII of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

203. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and the Class, the PII of Plaintiffs and the Class would not have been compromised.

204. There is a close causal connection between Defendants' failure to implement security measures to protect the PII of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The PII of Plaintiffs and the Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

205. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: INSERT

206. As a direct and proximate result of Defendants' negligence, Plaintiffs and the

Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

207. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession.

208. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

209. Defendants' negligent conduct is ongoing, in that it still holds the PII of Plaintiffs and Class Members in an unsafe and insecure manner.

210. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Breach of Third-Party Beneficiary Contract
(On Behalf of Plaintiffs and the Class against Defendant MESVision)

211. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein and brings this count solely against Defendant MESVision ("Defendant" for the purposes of this count).

212. Defendant entered into written contracts with its clients, including Costco, to provide eye care services to its clients' employees and other personnel.

213. In exchange, Defendant agreed, in part, to implement adequate security measures to safeguard the PII of Plaintiffs and the Class and to timely and adequately notify them of the Data Breach.

214. These contracts were made expressly for the benefit of Plaintiffs and the Class, as Plaintiffs and Class Members were the intended third-party beneficiaries of the contracts entered into between Defendant and its clients. Defendant knew that, if it were to breach these contracts with its clients, the clients' employees—Plaintiffs and Class Members—would be harmed.

215. Defendant breached the contracts it entered into with its clients by, among other things, failing to (i) use reasonable data security measures, (ii) implement adequate protocols and employee training sufficient to protect Plaintiffs' and Class Members' PII from unauthorized disclosure to third parties, and (iii) promptly and adequately notify Plaintiffs and Class Members of the Data Breach.

216. Plaintiffs and the Class were harmed by Defendant's breach of its contracts with its clients, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

217. Plaintiffs and Class Members are also entitled to their costs and attorney's fees incurred in this action.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiffs and the Class against Defendants)

218. Plaintiffs re-allege and incorporate by reference all preceding paragraphs, as if fully set forth herein, and bring this claim against both Defendants.

219. Plaintiffs and Class Members conferred a monetary benefit on Defendants. Specifically, they paid for or had payments made on their behalf for services from MESVision's

clients and/or provided labor to MESVision's clients as well as provided Defendants with their PII. In exchange, Plaintiffs and Class Members should have received from MESVision the services and/or the employment position from MESVision's clients that were the subject of the transaction and should have had their PII protected with adequate data security.

220. Defendants knew that Plaintiffs and Class Members conferred a benefit upon them and have accepted and retained that benefit by accepting and retaining the PII entrusted to them. Defendants profited from Plaintiffs' retained data and used Plaintiffs' and Class Members' PII for business purposes.

221. Defendants failed to secure Plaintiffs' and Class Members' PII and, therefore, did not fully compensate Plaintiffs or Class Members for the value that their PII provided.

222. Defendants acquired the PII through inequitable record retention as they failed to disclose the inadequate data security practices previously alleged.

223. If Plaintiffs and Class Members had known that Defendants would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their PII, they would have entrusted their PII at Defendants, obtained employment at MESVision's clients, and/or obtained services at MESVision.

224. Plaintiffs and Class Members have no adequate remedy at law.

225. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiffs and Class Members conferred upon it.

226. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: INSERT

227. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and

other compensation obtained by Defendants from their wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

228. Plaintiffs and Class Members may not have an adequate remedy at law against Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendants and that the Court grants the following:

- A. For an Order certifying this action as a class action and appointing Plaintiffs and her counsel to represent the Class, pursuant to Federal Rule of Civil Procedure 23;
- B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;
- C. For injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:
 - i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;
 - ii. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all

applicable regulations, industry standards, and federal, state or local laws;

- iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;
- iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;
- v. prohibiting Defendants from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;
- vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;
- vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- viii. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures; requiring Defendants to segment data by, among other things, creating firewalls and access

- controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;
- ix. requiring Defendants to conduct regular database scanning and securing checks;
 - x. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;
 - xi. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
 - xii. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendants' policies, programs, and systems for protecting personal identifying information;
 - xiii. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats,

both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

- xiv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;
- xv. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and
- xvi. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

- D. For an award of actual damages, compensatory damages, statutory damages, and nominal damages, in an amount to be determined, as allowable by law;
- E. For an award of punitive damages, as allowable by law;
- F. For an award of attorneys' fees and costs, and any other expenses, including expert witness fees;
- G. Pre- and post-judgment interest on any amounts awarded; and
- H. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

DATED: November 29, 2023

Respectfully submitted,

/s/ Randi Kassan.

Randi Kassan

MILBERG COLEMAN BRYSON

PHILLIPS GROSSMAN, LLC

100 Garden City Plaza

Garden City, NY 11530

Telephone: (212) 594-5300

rkassan@milberg.com

Counsel for Plaintiffs and the Proposed Class